TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire	**POUR SUITE A DONNER** voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale No. PCT/IB 03/04121	Date du dépôt international *(jour/mois/année)* 19.09.2003	Date de priorité *(jour/mois/année)* 27.09.2002
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04N7/167		
Déposant NAGRAVISION SA et.al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 5 feuilles, y compris la présente feuille de couverture.

   ☒ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

   Ces annexes comprennent 4 feuilles.

3. Le présent rapport contient des indications et les pages correspondantes relatives aux points suivants :

   - I ☒ Base de l'opinion
   - II ☐ Priorité
   - III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
   - IV ☐ Absence d'unité de l'invention
   - V ☒ Déclaration motivée selon la règle 66.2(a)(ii) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
   - VI ☐ Certains documents cités
   - VII ☐ Irrégularités dans la demande internationale
   - VIII ☐ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale	Date d'achèvement du présent rapport
13.04.2004	13.09.2004
Nom et adresse postale de l'adminstration chargée de l'examen préliminaire international Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Schneiderlin, J N° de téléphone +49 89 2399-7400

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/IB 03/04121

I. Base du rapport

1. En ce qui concerne les **éléments** de la demande internationale *(les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées, dans le présent rapport, comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17))* :

Description, Pages

1-15 telles qu'initialement déposées

Revendications, No.

1-12 reçue(s) le 12.08.2004 avec lettre du 29.07.2004

Dessins, Feuilles

1/1 telles qu'initialement déposées

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

   Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: ,qui est:

   ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).

   ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).

   ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés**divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

   ☐ contenu dans la demande internationale, sous forme écrite.

   ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.

   ☐ remis ultérieurement à l'administration, sous forme écrite.

   ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listages des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

   ☐ de la description, pages :

   ☐ des revendications, nos :

   ☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

   (Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport.)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui:	Revendications	1-12
	Non:	Revendications	
Activité inventive	Oui:	Revendications	1-12
	Non:	Revendications	
Possibilité d'application industrielle	Oui:	Revendications	1-12
	Non:	Revendications	

2. Citations et explications

   voir feuille séparée

Concernant le point V

Déclaration motivée quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

Il est fait référence au document suivant:

D1: 'FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM' EBU REVIEW- TECHNICAL, EUROPEAN BROADCASTING UNION. BRUSSELS, BE, no. 266, 21 décembre 1995 (1995-12-21), pages 64-77, XP000559450 ISSN: 0251-0936

Le document **D1** décrit (les références entre parenthèses s'appliquent à ce document) un système de déchiffrement de données à accès conditionnel, ce système mettant en oeuvre (voir figure 6) :

- un centre de diffusion (MUX, Scrambler, Modulator) agencé pour diffuser des données (picture, sound, data) chiffrées par un mot de contrôle (cw),
- un centre de gestion (Subcriber Authorisation System, Encrypter) agencé pour diffuser des messages personnels (ECM, EMM) relatifs à la gestion des moyens d'accès aux données chiffrées,
- un dispositif d'exploitation (DEMUX) destiné à rendre utilisables lesdites données chiffrées, et
- un décodeur agencé pour déchiffrer les données chiffrées, placé entre le centre de diffusion et le dispositif d'exploitation, formé de modules physiquement distincts :
  - un module de réception et de déchiffrement (Decrambler) des données chiffrées connecté au dispositif d'exploitation et
  - un module de gestion des droits d'accès (Conditonnal Access subsystem) à ces données, agencé pour communiquer avec le module de réception.

De plus le module de gestion comporte un module de sécurité (Security processor) comprenant un numéro d'identification unique (voir page 75 "customer's ID card" au milieu de la colonne de gauche) et des données (Keys) permettant de sécuriser la liaison entre ledit centre de gestion et le module de sécurité. Ce module de sécurité est agencé pour vérifier le contenu des messages personnels et pour permettre ou empêcher le déchiffrement du ou des mots de contrôle en fonction du contenu des messages personnels (voir page 75 colonne de gauche et note 1 et 2 de la figure 6). Et le module de réception reçoit les données chiffrées provenant du centre de diffusion via une première voie de communication (Tx, Rx, demodulator), et le module de gestion reçoit les messages personnels par le centre de gestion via une deuxième voie de communication (EMM via telephone ligne).

Par conséquent, l'objet de la revendication 1 diffère de D1 en ce que le module de gestion peut être mis en relation avec plusieurs centres de gestions.

Le document D1 mentionne l'utilisation de plusieurs centres de gestions (SAS I et J dans la figure 3) mais le module de gestion associé à un utilisateur n'est capable de communiqué qu'avec un seul centre de gestion (voir page 67 en haut de la colonne de gauche).

L'objet de la revendication 1 est donc nouveau (article 33(2) PCT).

Le problème que la présente invention se propose de résoudre peut donc être considéré comme augmenter la flexibilité du système de D1.

Aucun des documents disponibles ne suggère un module de gestion pouvant être mis en relation avec plusieurs centres de gestions.

La solution de ce problème proposée dans la revendication 1 de la présente demande est donc considérée comme impliquant une activité inventive (article 33(3) PCT).

Les revendications 2-12 dépendent de la revendication 1 et satisfont donc également, en tant que telles, aux conditions requises par le PCT en ce qui concerne la nouveauté et l'activité inventive.

REVENDICATIONS

1. Système de déchiffrement de données à accès conditionnel, ce système mettant en œuvre :

- un centre de diffusion (10) agencé pour diffuser des données chiffrées par au moins un mot de contrôle (cw),
- au moins deux centres de gestion (11) agencés pour diffuser des messages personnels (ECM, EMM) relatifs à la gestion des moyens d'accès aux données chiffrées,
- un dispositif d'exploitation (12) destiné à rendre utilisables lesdites données chiffrées, et
- un décodeur (13) agencé pour déchiffrer au moins une partie des données chiffrées, placé entre le centre de diffusion (10) et le dispositif d'exploitation (12),

caractérisé en ce que

- le décodeur (13) est formé d'un module de réception et de déchiffrement (14) des données chiffrées et d'un module de gestion (15) des droits d'accès à ces données, ces modules étant physiquement distincts, le module de réception (14) étant connecté au dispositif d'exploitation (12) et le module de gestion (15) étant agencé pour communiquer avec le module de réception,
- en ce que le module de gestion (15) comporte un module de sécurité (16) comprenant un numéro d'identification unique (UA) et des données permettant de sécuriser la liaison entre les centres de gestion (11) et le module de sécurité (16), ce module de sécurité étant agencé pour vérifier le contenu des messages personnels (ECM, EMM) et pour permettre ou empêcher le déchiffrement du ou des mots de contrôle (cw) en fonction du contenu des messages personnels,
- en ce que le module de réception (14) reçoit les données chiffrées provenant desdits centres de diffusion (10) via une première voie de communication, et le module de gestion (15) reçoit les messages

personnels (ECM, EMM) par le centre de gestion (11) via une deuxième voie de communication

- et en ce que le module de gestion comprend des données propres auxdits centres de gestion (11) avec lesquels il est apte à communiquer.

2. Système de déchiffrement de données selon la revendication 1, caractérisé en ce que la communication entre le module de réception (14) et le module de gestion (15) est une communication par ondes.

3. Système de déchiffrement de données selon la revendication 1, caractérisé en ce que le module de gestion (15) des droits est un téléphone portable.

4. Système de déchiffrement de données selon la revendication 3, caractérisé en ce que le module de sécurité (16) comprend des fonctions d'identification nécessaires à la téléphonie, et au moins une zone mémoire propre à un centre de gestion (11), cette zone comprenant les paramètres de sécurité pour la réception des messages d'autorisation (EMM) dudit centre de gestion.

5. Système selon les revendications 1 à 4, caractérisé en ce que le centre de diffusion (10) est agencé pour diffuser des messages de contrôle (ECM) comprenant le ou les mots de contrôle (cw), et en ce que les messages personnels diffusés par le centre de gestion (11) correspondent à un message d'autorisation (EMM).

6. Système selon les revendications 1 à 4, caractérisé en ce que le centre de gestion (11) est agencé pour diffuser des messages personnels comprenant le ou les mots de contrôle (cw), le module de sécurité (16) du module de gestion (15) disposant des moyens pour déterminer si ce message lui est destiné et de moyens pour transmettre ce mot de contrôle (cw) au module de réception (14).

7. Système selon la revendication 6, caractérisé en ce que le module de réception et de déchiffrement (14) comprend une clé unique de décryption appliquée au mot de contrôle (cw), cette clé servant à encrypter les mots de contrôle au centre gestion (11) avant leur transmission vers le module de gestion (15).

8. Système de déchiffrement de données selon la revendication 1, comportant au moins deux centres de gestion (11), caractérisé en ce que le module de sécurité (16) du module de gestion (15) comporte des paramètres de sécurité pour la réception des messages d'autorisation (EMM) provenant de centres de gestion (11) distincts.

9. Système de déchiffrement de données selon les revendications 1 à 8, le centre de diffusion (10) étant agencé pour transmettre des informations descriptives des données chiffrées, caractérisé en ce que ces données contiennent des indications nécessaires à l'établissement d'une communication avec le centre de gestion (11) en charge de l'autorisation de ces données, et sont transmises au module de gestion (15), ce dernier étant agencé pour établir une communication avec le centre de gestion (11) concerné pour l'obtention du message d'autorisation (EMM) .

10. Système de déchiffrement de données selon l'une des revendications précédentes, caractérisé en ce que le module de réception et de déchiffrement (14) est intégré dans le dispositif d'exploitation (12).

11. Système de déchiffrement de données selon la revendication 1, caractérisé en ce que le module de réception et de déchiffrement (14) comprend des moyens de communication standardisé avec le module de gestion (15) de sorte qu'un module de réception et de déchiffrement (14) puisse dialoguer avec une pluralité de modules de gestion (15).

12. Système de déchiffrement de données selon l'une des revendications précédentes, caractérisé en ce que le module de gestion

(15) comprend des moyens pour établir une clé d'appariement avec le module de réception (14), cette clé étant destinée à encrypter et décrypter au moins le ou les mots de contrôle (cw) transmis du module de gestion (15) vers le module de réception (14).

5